PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-103048
(43)Date of publication of application : 13.04.2001

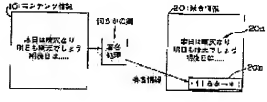
(51)Int.Cl. H04L 9/32
G06F 12/14
G09C 5/00
H04N 1/387

(21)Application number : 11-273949
(22)Date of filing : 28.09.1999

(71)Applicant : FUJITSU LTD
(72)Inventor : KOTANI MASATAKE
HASEBE TAKAYUKI
AKIYAMA RYOTA
SASAKI TAKAOKI

(54) METHOD AND DEVICE FOR MANAGING INFORMATION AND INFORMATION MANAGEMENT PROGRAM STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To give a sense of security that contents information is true to a user, about an information managing method or the like which manages digitized contents information.
SOLUTION: This information managing device generates signature information by subscribing one's name on the contents information 10 with a signature key, generates integrated information 20 obtained by uniting the contents information and the signature information into one and displays or outputs the form of the integrated information 20 as is, in the case of displaying or outputting the integrated information 20.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－103048
（P2001－103048A）
(43)公開日　平成13年４月13日（2001.4.13）

(51)Int.Cl.'	識別記号	Ｆ Ｉ		ﾃｰﾏｺｰﾄﾞ（参考）
Ｈ０４Ｌ　9/32		Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ０９Ｃ　5/00		５Ｃ０７６
Ｇ０９Ｃ　5/00		Ｈ０４Ｎ　1/387		５Ｊ１０４
Ｈ０４Ｎ　1/387		Ｈ０４Ｌ　9/00	６７３Ｄ	９Ａ００１

審査請求　未請求　請求項の数17　ＯＬ　（全 12 頁）

(21)出願番号　特願平11－273949

(22)出願日　平成11年９月28日(1999.9.28)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　小谷　誠剛
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

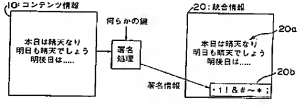
(72)発明者　長谷部　高行
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(74)代理人　100094330
弁理士　山田　正紀

最終頁に続く

(54)【発明の名称】　情報管理方法、情報管理装置、および情報管理プログラム記憶媒体

(57)【要約】
【課題】本発明は、ディジタル化されたコンテンツ情報を管理する情報管理方法等に関し、コンテンツ情報が真正なものであるという安心感をユーザに与える。
【解決手段】コンテンツ情報１０を署名鍵で署名して署名情報を生成し、そのコンテンツ情報と署名情報を一体化した統合情報２０を生成し、表示やプリント出力にあたっては、その統合情報２０の形態のまま表示あるいは出力を行なう。



1

【特許請求の範囲】

【請求項１】　コンテンツ情報に署名鍵で署名することにより署名情報を生成し、

該コンテンツ情報と該署名情報を、視覚的に一体化された統合情報に統合することを特徴とする情報管理方法。

【請求項２】　所定の秘密情報に基づいて署名鍵を生成し、この生成された署名鍵でコンテンツ情報に署名することを特徴とする請求項１記載の情報管理方法。

【請求項３】　所定の可視情報を二次元ビットマップに変換することにより二次元情報を生成し、この生成された二次元情報と所定の秘密情報とに基づいて署名鍵を生成し、この生成された署名鍵でコンテンツ情報に署名することを特徴とする請求項１記載の情報管理方法。

【請求項４】　前記可視情報が手書きされた情報であることを特徴とする請求項３記載の情報管理方法。

【請求項５】　前記可視情報が押印された情報であることを特徴とする請求項３記載の情報管理方法。

【請求項６】　コンテンツ情報への署名に代えて、コンテンツ情報に所定の付加情報を付加した情報に署名鍵で署名し、該コンテンツ情報と該署名鍵とさらに該付加情報とを統合することによって、視覚的に一体化された統合情報を生成することを特徴とする請求項１記載の情報管理方法。

【請求項７】　コンテンツ情報に時刻情報を付加し、時刻情報が付加されたコンテンツ情報に署名鍵で署名することを特徴とする請求項１記載の情報管理方法。

【請求項８】　前記統合情報からコンテンツ情報と署名情報を分離するとともに、該統合情報から分離されたコンテンツ情報に署名鍵で署名することにより検証用署名情報を生成し、この生成された検証用署名情報と、前記統合情報から分離された署名情報とを比較することを特徴とする請求項１記載の情報管理方法。

【請求項９】　所定の秘密情報に基づいて署名鍵を生成し、この生成された署名鍵で、前記統合情報から分離されたコンテンツ情報に署名することを特徴とする請求項８記載の情報管理方法。

【請求項１０】　所定の可視情報を二次元ビットマップに変換することにより二次元情報を生成し、この生成された二次元情報と所定の秘密情報とに基づいて署名鍵を生成し、この生成された署名鍵で、前記統合情報から分離されたコンテンツ情報に署名することを特徴とする請求項８記載の情報管理方法。

【請求項１１】　前記統合情報から分離された署名情報と、該統合情報から分離されたコンテンツ情報に署名鍵で署名することにより得られた検証用署名情報とを比較した結果これら双方の署名情報が一致した場合に、該統合情報へのアクセスを許容することを特徴とする請求項８記載の情報管理方法。

【請求項１２】　コンテンツ情報に署名鍵で署名することにより署名情報を生成する署名手段と、

2

前記署名手段により署名されたコンテンツ情報と該署名により生成された署名情報を、視覚的に一体化された統合情報に統合する統合手段とを備えたことを特徴とする情報管理装置。

【請求項１３】　前記統合情報からコンテンツ情報と署名情報を分離する分離手段と、

該統合情報から分離されたコンテンツ情報に署名鍵で署名することにより検証用署名情報を生成する検証用署名手段と、

該検証用署名手段で生成された検証用署名情報と、前記分離手段により前記統合情報から分離された署名情報とを比較する比較手段とを備えたことを特徴とする請求項１２記載の情報管理装置。

【請求項１４】　前記比較手段は、前記分離手段により前記統合情報から分離された署名情報と、前記検証用署名手段により生成された検証用署名情報とを比較した結果これら双方の署名情報が一致した場合に、該統合情報へのアクセスを許容するものであることを特徴とする請求項１３記載の情報管理装置。

【請求項１５】　コンテンツ情報に署名鍵で署名することにより署名情報を生成する署名手段と、

前記署名手段により署名されたコンテンツ情報と該署名により生成された署名情報を、視覚的に一体化された統合情報に統合する統合手段とを有する情報管理プログラムが記憶されていることを特徴とする情報管理プログラム記憶媒体。

【請求項１６】　前記情報管理プログラムは、

前記統合情報からコンテンツ情報と署名情報を分離する分離手段と、

該統合情報から分離されたコンテンツ情報に署名鍵で署名することにより検証用署名情報を生成する検証用署名手段と、

該検証用署名手段で生成された検証用署名情報と、前記分離手段により前記統合情報から分離された署名情報とを比較する比較手段とを、さらに有するものであることを特徴とする請求項１５記載の情報管理プログラム記憶媒体。

【請求項１７】　前記比較手段は、前記分離手段により前記統合情報から分離された署名情報と、前記検証用署名手段により生成された検証用署名情報とを比較した結果これら双方の署名情報が一致した場合に、該統合情報へのアクセスを許容するものであることを特徴とする請求項１６記載の情報管理プログラム記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ディジタル化されたコンテンツ情報を管理する情報管理方法、情報管理装置、および、コンピュータあるいはコンピュータシステムをそのような情報管理装置として機能させるための情報管理プログラムが記憶された情報管理プログラム記憶

媒体に関する。

【０００２】

【従来の技術】コンテンツ情報のディジタル化が時代の趨勢となってきている。ディジタル化されたコンテンツ情報に署名鍵でディジタル署名を行ない署名情報を生成することが容易になり、その署名情報をコンテンツ情報に対応づけて運用することが盛んに行なわれるようになってきている。

【０００３】ディジタル署名によって生成される署名情報はコンテンツ情報に依存した情報であり、異なるコンテンツ情報からは異なる署名情報が生成される。例えば修正あるいは改ざんされたコンテンツ情報にディジタル署名を行なったとき、生成される署名情報がその修正あるいは改ざんによってどのように変化するかを予想することは極めて困難である。この性質を利用し、例えばそのコンテンツ情報と署名情報を送信して、それらを受信した側でその受信したコンテンツ情報を同じ署名鍵で再度署名して署名情報を生成し、その生成した署名情報と受信した署名情報とを比較することにより、そのコンテンツ情報が修正あるいは改ざんのない真正なものであるかどうかを調べることができる。

【０００４】

【発明が解決しようとする課題】コンテンツ情報の修正や改ざんの有無の検出自体については、上記のような署名情報を用いることによって可能であるが、この検出作業はコンピュータ等の内部のユーザからは見えない部分で行なわれるため、修正や改ざんのない、確かに真正なコンテンツ情報であるという安心感をユーザに与えにくいという、感覚的な面で問題がある。

【０００５】古来、印影や手書きサインで本人認証をしてきた長い歴史がありそれが文化として醸立している中では、コンピュータ等の内部で自分には見えないところで処理されてこれは真正なものであるという結果だけ情報を与えられることに対し違和感を抱く人々が多数存在することも否定できない。

【０００６】手書き文字（サイン）を入力してその手書き文字を基に署名鍵を作成することが提案されており（特開平７－２６２３７２号公報参照）、これを採用すると、コンテンツ情報を作成した側にそのコンテンツ情報に確かに署名したという一種の安心感を与える効果はあるが、そのコンテンツ情報を利用する側における、そのコンテンツ情報が真正なものであるという納得がいま一つ十分でないという問題点を解決するものではない。

【０００７】本発明は、上記事情に鑑み、コンテンツ情報が真正なものであるという安心感をユーザに与えることのできる情報管理を実現する情報管理方法、その情報管理方法を実行する情報管理装置、および、コンピュータあるいはコンピュータシステムで実行されることによりそのような情報管理を実現する情報管理プログラムが記憶された情報管理プログラム記憶媒体を提供することを目的とする。

【０００８】

【課題を解決するための手段】上記目的を達成する本発明の情報管理方法は、コンテンツ情報に署名鍵で署名することにより署名情報を生成し、そのコンテンツ情報とその署名情報を、視覚的に一体化された統合情報に統合することを特徴とする。

【０００９】ここで、上記の「視覚的に一体化された」とは、画面表示や用紙上へのプリント出力の際に、一体化された情報として表示ないし出力されることをいう。典型的にはそのコンテンツ情報と署名情報が一体的に１つのファイルに格納されていることをいうが、コンテンツ情報と署名情報が別々のファイルを構成し、画面表示あるいはプリント出力にあたって1つとかたまりの情報として表示ないし出力されるように構成したものであってもよい。

【００１０】本発明の情報管理方法によれば、コンテンツ情報と署名情報が、例えば表示画面上への表示あるいは用紙上へのプリント出力等の場合に、視覚的に一体化された統合情報に統合されているため、その統合情報として一体化された署名情報が、心理上、長い歴史の中で培ってきた印影やサインと同様の役割りを果たし、ユーザに安心感を与えることができる。

【００１１】また、コンテンツ情報は表示画面上でのみ確認する場合も多いが、そのコンテンツ情報が重要な情報であればあるほど用紙上にプリント出力してそのコンテンツ情報を保存しあるいは利用することも多い。そのような場合、本発明によれば、用紙上にコンテンツ情報のみでなく署名情報も記録されているためそのコンテンツ情報が真正なものであることを確認する必要を生じたときはその用紙上の記録をＯＣＲ（光学的な文字入力装置）により読み込ませその読み込ませた統合情報から署名情報を分離して検証に用いることができる。実際にはプリント出力された全てのものについて上記のようなＯＣＲで読み込ませて検証するという作業を行なわなくても、プリント出力されたものからも真正であることを検証する方法が存在するということをもってユーザに大きな安心感を与えることができる。

【００１２】ここで、上記本発明の情報管理方法において、所定の秘密情報に基づいて署名鍵を生成し、この生成された署名鍵でコンテンツ情報に署名することが好ましい。

【００１３】上記の「所定の秘密情報」は、特定のものに限られるものではないが、典型的には、この情報管理方法の実施がある１台のコンピュータ内で完結しているときはそのコンピュータにユニークな装置番号等をいい、あるいは、この情報管理方法がある１つのシステムに加入している加入者間で共用されるときはそのシステムの加入者にのみ通知されるパスワード等をいう。

【００１４】このように、署名情報の生成時に使用する

署名鍵を、システムあるいは装置の秘密情報から生成することにより、同一のコンテンツ情報を別システムあるいは別装置にて処理する場合において署名情報を異なるものとすることができ、したがって署名情報のユニーク性を高めることができる。

【００１５】また、上記本発明の情報管理方法において、所定の可視情報を二次元ビットマップに変換することにより二次元情報を生成し、この生成された二次元情報と所定の秘密情報とに基づいて署名鍵を生成し、この生成された署名鍵でコンテンツ情報に署名することも好ましい態様である。ここで、上記可視情報は手書きされた情報であってもよく、あるいは、上記可視情報は押印された情報であってもよく、その他の可視情報（例えばあるシステムの加入者あるいはあるグループの構成員であることを表わすマークや文字等）であってもよい。

【００１６】このように、秘密情報に加えて可視情報から作成された二次元情報を用いて署名鍵を生成すると署名情報のユニーク性を一層高めることができる。この場合において、手書きされた情報や押印された情報を可視情報として使用すると、従来から慣習として行なわれてきた手書きサイン認証や捺印認証と親和性とのある署名認証を行なうことができる。

【００１７】さらに、上記本発明の情報管理方法において、コンテンツ情報への署名に代えて、コンテンツ情報に所定の付加情報を付加した情報に署名鍵で署名し、そのコンテンツ情報とその署名鍵とさらにその付加情報とを統合することによって、視覚的に一体化された統合情報を生成することも好ましい。

【００１８】この「付加情報」は特定の情報に限定されるものではないが、例えば署名時点における時刻情報、あるいは作成されたコンテンツ情報の内容を承認した承認者（例えば会社におけるある部署の責任者）の名前等であってもよい。

【００１９】このように、コンテンツ情報に、そのコンテンツ情報とは別の概念としての付加情報を付加して署名することにより、コンテンツ情報に署名した時刻や承認署名等を明確にすることができ、また、後の署名照合等においてその付加情報を運用することができる。

【００２０】また、上記本発明の情報管理方法において、コンテンツ情報に時刻情報を付加し、時刻情報が付加されたコンテンツ情報に署名鍵で署名することも好ましい形態である。

【００２１】この「時刻情報」は特定のものに限られるものではなく、例えばコンテンツ情報作成時の時刻を表わす時刻情報であってもよく、あるいは署名時の時刻であってもよい。

【００２２】このようにコンテンツ情報に時刻情報を付加しその時刻情報が付加された情報をコンテンツ情報として取り扱うことによっても、上述のコンテンツ情報とは別に付加情報を付加する場合と同様、そのコンテンツ情報の作成時刻あるいは署名時刻を明確にすることができる。

【００２３】さらに、本発明の情報管理方法において、コンテンツ情報が真正のものであるかどうか検証する必要があるときは、上記統合情報からコンテンツ情報と署名情報を分離するとともに、その統合情報から分離されたコンテンツ情報に署名鍵で署名することにより検証用署名情報が生成され、この生成された検証用署名情報と、上記統合情報から分離された署名情報とが比較される。

【００２４】本発明では、署名情報が人の目に見える形でコンテンツ情報と統合されて統合情報となっているため、署名照合の処理に用いられる情報を把握することが容易であり、かつ、上記のようにしてコンテンツ情報が真正なものであることを検証する方法を確立しておくことにより、ユーザの安心感が一層高められる。

【００２５】さらに、この検証時においても、所定の秘密情報に基づいて署名鍵を生成し、この生成された署名鍵で、上記統合情報から分離された署名情報に署名することが好ましく、所定の可視情報を二次元ビットマップに変換することにより二次元情報を生成し、この生成された二次元情報と所定の秘密情報とに基づいて署名鍵を生成し、この生成された署名鍵で、上記統合情報から分離されたコンテンツ情報に署名することがさらに好ましい。

【００２６】システムまたは装置の秘密情報から署名鍵を生成することにより、あるいはその秘密情報と、可視情報から作成された二次元情報とから署名鍵を作成することにより、前述したように、署名情報のユニーク性を高めることができる。

【００２７】ここで、統合情報から分離された署名情報と、その統合情報から分離されたコンテンツ情報に署名鍵で署名することにより得られた検証用署名情報とを比較した結果これら双方の署名情報が一致した場合に、その統合情報へのアクセスを許容することにより、改ざんあるいはデータエラーの可能性のあるコンテンツ情報へのアクセスを防止することができる。

【００２８】また、上記目的を達成する本発明の情報管理装置は、コンテンツ情報に署名鍵で署名することにより署名情報を生成する署名手段と、その署名手段により署名されたコンテンツ情報とその署名により生成された署名情報を、視覚的に一体化された統合情報に統合する統合手段とを備えたことを特徴とする。

【００２９】この情報管理装置において、さらに上記統合情報からコンテンツ情報と署名情報を分離する分離手段と、その統合情報から分離されたコンテンツ情報に署名鍵で署名することにより検証用署名情報を生成する検証用署名手段と、検証用署名手段で生成された検証用署名情報と、分離手段により統合情報から分離された署名情報とを比較する比較手段とを備えたことを特徴とす

る。

【００３０】この場合に、上記比較手段は、分離手段により統合情報から分離された署名情報と、検証用署名手段により生成された検証用署名情報とを比較した結果これら双方の署名情報が一致した場合に、その統合情報へのアクセスを許容するものであることが好ましい。

【００３１】また、上記目的を達成する本発明の情報管理プログラム記憶媒体は、コンテンツ情報に署名鍵で署名することにより署名情報を生成する署名手段と、その署名手段により署名されたコンテンツ情報とその署名により生成された署名情報を、視覚的に一体化された統合情報に統合する統合手段とを有する情報管理プログラムが記憶されていることを特徴とする。

【００３２】この情報管理プログラムは、上記統合情報からコンテンツ情報と署名情報を分離する分離手段と、その統合情報から分離されたコンテンツ情報に署名鍵で署名することにより検証用署名情報を生成する検証用署名手段と、その検証用署名手段で生成された検証用署名情報と、分離手段により統合情報から分離された署名情報とを比較する比較手段とを、さらに有するものであることが好ましい。

【００３３】この場合に、上記比較手段は、分離手段により統合情報から分離された署名情報と、検証用署名手段により生成された検証用署名情報とを比較した結果これら双方の署名情報が一致した場合に、その統合情報へのアクセスを許容するものであることが好ましい。

【００３４】尚、本発明の情報管理装置と本発明の情報管理プログラム記憶媒体に記憶された情報管理プログラムとの双方で「手段」という用語を用いているが、情報管理装置における手段は、ハードウェアとソフトウェアとの組合せをいい、情報管理プログラムの場合は、そのうちのソフトウェアの部分のみを手段と称している。

【００３５】

【発明の実施の形態】以下、本発明の実施形態について説明する。

【００３６】図１は、本発明の情報管理装置の一実施形態を構成するパーソナルコンピュータの外観斜視図である。このパーソナルコンピュータには、本発明にいう情報管理プログラムの一実施形態がインストールされて実行されることにより、本発明の一実施形態としての情報管理方法が実施される。

【００３７】このパーソナルコンピュータ１００は、ＣＰＵ、ＲＡＭ、ハードディスク等を内蔵した本体部１０１、本体部１０１からの指示により表示画面１０２ａに画面表示を行うＣＲＴディスプレイ１０２、このパーソナルコンピュータにユーザの指示や文字情報を入力するためのキーボード１０３、表示画面１０２ａ上の任意の位置を指定することによりその位置に表示されていたアイコン等に応じた指示を入力するマウス１０４を備えている。

【００３８】本体部１０１は、さらに、外観上、フロッピディスク２１２（図１には図示せず；図２参照）やＣＤＲＯＭ２１０が取り出し自在に装填されるフロッピディスク装填口１０１ａおよびＣＤＲＯＭ装填口１０１ｂを有しており、その内部には、装填されたフロッピディスクやＣＤＲＯＭ２１０をドライブする、フロッピディスクドライバ２２４、ＣＤＲＯＭドライバ２２５（図２参照）も内蔵されている。

【００３９】ここでは、ＣＤＲＯＭ２１０に、本発明にいう情報管理プログラムの一例が記憶されている。このＣＤＲＯＭ２１０がＣＤＲＯＭ装填口１０１ｂから本体部１０１内に装填され、ＣＤＲＯＭドライバ２２５により、そのＣＤＲＯＭ２１０に記憶された情報管理プログラムがこのパーソナルコンピュータ１００のハードディスク内にインストールされる。

【００４０】この情報管理プログラムが記憶されたＣＤＲＯＭは、本発明の情報管理プログラム記憶媒体の一実施形態に相当する。

【００４１】また、このＣＤＲＯＭに記憶された情報管理プログラムは、上記のようにしてパーソナルコンピュータ１００のハードディスク内にインストールされるが、その情報管理プログラムがインストールされた状態のハードディスクも、本発明の情報管理プログラム記憶媒体の一実施形態に相当する。

【００４２】さらに、その情報管理プログラムがフロッピディスク等にダウンロードされるときは、そのダウンロードされた情報管理プログラムを記憶した状態にあるフロッピディスク等も、本発明の情報管理プログラム記憶媒体の一実施形態に相当する。

【００４３】図２は、図１に外観を示すパーソナルコンピュータのハードウェア構成図である。

【００４４】ここには、中央演算処理装置（ＣＰＵ）２２１、ＲＡＭ２２２、ハードディスクコントローラ２２３、フロッピディスクドライバ２２４、ＣＤＲＯＭドライバ２２５、マウスコントローラ２２６、キーボードコントローラ２２７、およびディスプレイコントローラ２２８が示されており、それらはバス２２０で相互に接続されている。

【００４５】フロッピディスクドライバ２２４、ＣＤＲＯＭドライバ２２５は、図１を参照して説明したように、それぞれフロッピディスク２１２、ＣＤＲＯＭ２１０が装填され、装填されたフロッピディスク２１２、ＣＤＲＯＭ２１０をアクセスするものである。

【００４６】図３は、ＣＤＲＯＭに記憶された情報管理プログラムの一例を示す図である。

【００４７】この図３に示すように、ＣＤＲＯＭ２１０は、署名手段２５１、統合手段２５２、分離手段２５３、検証用署名手段２５４、および比較手段２５５を有する情報管理プログラム２５０が記憶されている。各手段２２１～２２５の詳細については後述する。

【００４８】図４は、本発明にいう情報管理プログラムが動作するもう１つの環境であるコンピュータネットワークを示す図である。

【００４９】この図４には、コンピュータネットワークを構成するコンピュータシステムとして２台のクライアントマシン３００，４００と１台のサーバマシン５００が例示されており、これらのコンピュータシステム３００，４００，５００は通信網６００を介して互いに接続されている。

【００５０】各クライアントマシン３００，４００およびサーバマシン５００は、基本的には図１，図２に示すパーソナルコンピュータに通信の機能を付加した構成を備えている。すなわち、各クライアントマシン３００，４００およびサーバマシン５００は、ＣＰＵ、主記憶装置、ハードディスク、通信用ボード等が内蔵された本体部３０１，４０１，５０１、本体部３０１，４０１，５０１からの指示により表示画面３０２ａ，４０２ａ，５０２ａ上に画像や文字列を表示する表示部３０２，４０２，５０２、本体部３０１，４０１，５０１にユーザの指示を入力するためのキーボード３０３，４０３，５０３、表示画面３０２ａ，４０２ａ，５０２ａ上の任意の位置を指定することにより、その指定時にその位置に表示されていたアイコン等に応じた指示を入力するマウス３０４，４０４，５０４を備えている。

【００５１】また、各本体部３０１，４０１，５０１には、さらに外観上、フロッピィディスクが装填されるＦＤ装填口３０１ａ，４０１ａ，５０１ａ、ＣＤＲＯＭ装填口３０１ｂ，４０１ｂ，５０１ｂを有しており、それらの内部には、それらの装填口３０１ａ，３０１ｂ；４０１ａ，４０１ｂ；５０１ａ，５０１ｂから装填されたフロッピィディスクやＣＤＲＯＭをドライブしてアクセスする、フロッピィディスクドライバ、ＣＤＲＯＭドライバにも内蔵されている。

【００５２】サーバマシン５００は、クライアントマシン３００，４００のホストコンピュータとして働き、クライアントマシン３００，４００間で送受信される電子メール等のコンテンツ情報の送受信を仲介する。

【００５３】以下、図１に示すパーソナルコンピュータ内部、あるいは図４に示すコンピュータネットワーク内で実行される、本発明に沿った処理について説明する。ここでは、図１に示すパーソナルコンピュータを動作環境とする場合は、コンテンツ情報に署名して統合情報を生成する第１段階と、その統合情報中のコンテンツ情報が真正なものであるか否か検証を行なう第２段階との双方がそのパーソナルコンピュータで実行され、図４に示すコンピュータネットワークを動作環境とする場合は、上記の態様のほか、上述の第１段階はクライアントマシン３００，４００のうちのコンテンツ情報送信側のマシンで実行され、上述の第２段階はそれらのクライアントマシン３００，４００のうちの受信側のマシンで実行されるという態様も存在する。

【００５４】図５は、統合情報生成処理の第１例を示す模式図、図６は、その統合情報生成処理を表わすフローチャートである。

【００５５】ここでは先ずコンテンツ情報１０の入力が行なわれる（ステップＳ１）。コンテンツ情報の入手は、コンテンツ情報を新たに作成したりあるいは既に存在するコンテンツ情報を新たに修正あるいは編集して作成したものであってもよく、あるいは外部で作成されたコンテンツ情報を入手したものであってもよい。

【００５６】次にそのコンテンツ情報１０に署名するための署名鍵の入手が行なわれる（ステップＳ２）。この署名鍵は、既に記憶しておいたものを読み出してもよく、あるいはユーザによりパスワード等として入力されるものであってもよく、ここではその署名鍵の入手方法の如何を問うものではない。

【００５７】上記のようにコンテンツ情報と署名鍵が入手された後、そのコンテンツ情報１０にその署名鍵で署名処理が行なわれて署名情報が生成される（ステップＳ３）。この署名処理は、図３に示す情報処理プログラム２５０の署名手段２５１に相当する。

【００５８】次に、その生成された署名情報をコンテンツ情報と統合して統合情報２０を生成する（ステップＳ４）。この統合情報２０は、本発明で要請される要件としては、表示やプリント出力のときにコンテンツ情報と署名情報が視覚的に一体化されていればよいが、本実施形態では、表示や出力のときのみでなく、コンテンツ情報２０ａと署名情報２０ｂが全体として１つの情報として常に一体化された１つのファイルが作成される。この統合処理（ステップＳ４）は、図３に示す情報処理プログラム２５０における統合手段２５２に相当する。

【００５９】このようにコンテンツ情報と署名情報を一体化した統合情報を作成することにより、その統合情報中の署名情報が印影やサインと同様の役割を果たし、ユーザに安心感を与えることができる。

【００６０】図７は、統合情報生成処理の第２例を示す模式図、図８は、その第２例を実現するための、図６に示すフローチャートからの変更部分を示す部分フローチャートである。

【００６１】図７において図５と異なる点は、コンテンツ情報１０に署名処理を行なうための署名鍵が、システム又は装置内の秘密情報から作成されるものであるという点が明示されている点である。

【００６２】この場合、図８に示すように、図６の鍵入手のステップＳ２は、秘密情報入手のステップ２０１とその秘密情報に基づいて署名鍵を生成するステップＳ２０２で構成される。秘密情報としては、図１に示す動作環境の場合はそのパーソナルコンピュータの装置番号、図４に示す動作環境の場合はそのコンピュータネットワークにユニークなパスワード等を採用することができ

る。

【００６３】このように署名鍵を秘密情報に基づいて作成することにより、その署名鍵を用いて生成される署名情報のユニーク性を高めることができる。

【００６４】図９は、統合情報生成処理の第３例を示す模式図、図１０は、その第３例を実現するための、図６に示すフローチャートからの変更部分を示す部分フローチャートである。

【００６５】図９において図５とは異なる点は、可視情報が二次元処理により二次元のビットマップを表わす二次元情報に変換され、その二次元情報と秘密情報とに基づいて署名鍵が作成される点である。

【００６６】この場合、図１０に示すように、図６の鍵入手のステップＳ２は、可視情報入手のステップＳ２１１と、その入手した可視情報を二次元処理により二次元ビットマップに変換して二次元情報を生成するステップＳ２１２と、秘密情報を入手するステップＳ２１３と、それら二次元情報と秘密情報から署名鍵を生成するステップＳ２１４とで構成される。

【００６７】このように署名鍵を秘密情報のみでなく可視情報（二次元情報）にも基づいて作成することにより、その作成された署名鍵を用いて作成される署名情報のユニーク性が更に高められる。

【００６８】尚、この第３例における統合情報の生成にあたっては、署名を行なう前にコンテンツ情報に二次元情報を組み込むことにより二次元情報が組み込まれたコンテンツ情報を作成し、その二次元情報が組み込まれたコンテンツ情報に署名することにより得られる署名情報と、その二次元情報が組み込まれたコンテンツ情報とを統合してもよく、あるいは、二次元情報を組み込む前のコンテンツ情報に署名を行ない、その署名により生成された署名情報と、コンテンツ情報と、二次元情報とを統合してもよい。

【００６９】図１１は、図９，図１０を参照して説明した第３例の具体例を示す模式図である。図１０との相違点について説明する。

【００７０】この図１１には、手書き入力装置３１が示されており、ユーザがこの手書き入力装置３１を用いて自分のサインを入力する。するとそのサインを可視情報としてその可視情報について二次元処理が行なわれる。その他の点は、図９，図１０を参照して説明したとおりである。

【００７１】この場合、統合情報２０として、コンテンツ情報２０ａと署名情報２０ｂとの外に二次元情報２０ｃも一体的に統合された統合情報が生成される。

【００７２】図１２は、図９，図１０を参照して説明した第３例のもう１つの具体例を示す模式図である。

【００７３】この図１２には、二次元読み取り装置３２が示されており、ユーザは、自分の印鑑をその二次元読み取り装置３２に押印する動作を行なう。そうするとその二次元読み取り装置３２はその印影を読み取ってその印影が可視情報として入力される。その後の処理は図１１の場合と同様である。

【００７４】このように、可視情報として手書きサインや印影を使用すると、従来から行なわれてきた手書きサイン認証や捺印認証と親和性のある署名認証を行なうことができる。

【００７５】図１３は、統合情報生成処理の第４例を示す模式図、図１４はその第４例を実現するための、図６に示すフローチャートへの追加部分を示す部分フローチャートである。

【００７６】図１３における、図５に示す第１例との相違点は、付加情報を入手し、コンテンツ情報に付加情報を付加した情報を署名鍵で署名する点である。

【００７７】この場合、図６に示すフローチャート中のコンテンツ情報入手のステップ（ステップＳ１）と鍵入手のステップ（ステップＳ２）との間Ｐ１に、図１４に示す付加情報入手のステップ（ステップＳ５）が挿入される。また、この場合、図６の統合処理のステップ（ステップＳ４）では、コンテンツ情報２０ａと署名情報２０ｂとさらにその付加情報２０ｄとが統合されて統合情報２０が生成される。

【００７８】ここで、付加情報は、例えば時刻情報であってもよく、上述のサインや印影等の可視情報（二次元情報）であってもよく、上述の秘密情報に類した情報であってもよい。

【００７９】このようにコンテンツ情報に付加情報を付加して署名することにより、後の処理でその付加情報の有効利用を図ることができる。

【００８０】図１５は、統合情報生成処理の第５例を示す構成図、図１６はその第５例を実現するための、図６に示すフローチャートへの追加部分を示す部分フローチャートである。

【００８１】図１５における、図５に示す第１例との相違点は、コンテンツ情報に時刻情報が付加されてその時刻情報が付加されたコンテンツ情報が生成され、その時刻情報を含むコンテンツ情報に署名処理が行なわれる。この場合、図６に示すフローチャート中の、コンテンツ情報入手のステップ（ステップＳ１）と鍵入手のステップ（ステップＳ２）との間Ｐ１に、図１５に示す時刻情報入手のステップ（ステップＳ６）が挿入される。

【００８２】ここで、この時刻情報は、コンテンツ情報が作成された時点の時刻を表わす時刻情報であってもよくコンテンツ情報に署名を行なう時点の時刻情報であってもよい。

【００８３】このように時刻情報を付加することにより生成された、時刻情報を含むコンテンツ情報に署名し、その署名により得られた署名情報と、時刻情報を含むコンテンツ情報とを統合することにより、後の署名照合時等に時刻情報を運用することができる。

13

【００８４】次に、統合情報中のコンテンツ情報が真正なものであるか否かの検証を行なう検証処理について説明する。

【００８５】図１７は、検証処理の第１例を示す模式図、図１８はその検証処理の第１例を表わすフローチャートである。

【００８６】ここでは、先ず統合情報２０から署名情報とコンテンツ情報を分離する分離処理が行なわれる（ステップＳ７）。この分離処理は、図３に示す情報管理プログラム２５０の分離手段２５３に相当する。

【００８７】次に、前述した統合情報生成処理において使用した署名鍵と同一の署名鍵を入手し（ステップＳ８）、その入手した署名鍵を用いて、その統合情報から分離されたコンテンツ情報１０に署名処理を行ない検証用署名情報を生成する（ステップＳ９）。この検証用所署名情報を作成するための署名処理は、図３に示す情報管理プログラム２５０の検証用署名手段２５４に相当する。

【００８８】さらに、上記のように生成された検証用署名情報と、統合情報２０から分離された署名情報とを比較照合してそれらの一致不一致を検出する比較処理が行なわれる（ステップＳ１０）。この比較処理は、図３に示す情報管理プログラム２５０の比較手段２２５に相当する。

【００８９】このように、実際に検証を行なうことができるように構成しておくことにより、コンテンツ情報に一体化された署名情報に信頼を置くことができ、ユーザに一層の安心感を与えることができる。

【００９０】図１９は、検証処理の第２例を示す模式図、図２０は、その第２例を実現するための、図１８に示すフローチャートからの変更部分を示す部分フローチャートである。

【００９１】この場合、図２０に示すように、鍵入手のステップ（ステップＳ８）は、秘密情報入手のステップＳ８０１と、その入手した秘密情報に基づいて署名鍵を生成するステップＳ８０２とで構成される。この図１９，図２０に示す第２例は、図７，図８を参照して説明した統合情報生成処理の第２例に対応しており、その統合情報生成処理の第２例で入手される秘密情報と同一の秘密情報が入手され、その入手した秘密情報に基づいて、同一のアルゴリズムにより、その統合情報生成処理の第２例で生成された署名鍵と同一の署名鍵が生成される。

【００９２】図２１は、検証処理の第３例を示す模式図、図２２は、その第３例を実現するための、図１８に示すフローチャートからの変更部分を示す部分フローチャートである。

【００９３】この場合、図２２に示すように、図１８の鍵入手のステップＳ８は、可視情報入手のステップＳ８１１と、その入手した可視情報を二次元処理により二次元ビットマップに変換して二次元情報を生成するステップＳ８１２と、秘密情報を入手するステップＳ８１３と、それら二次情報と秘密情報から署名鍵を生成するステップＳ８１４とで構成される。

14

【００９４】この図２１，図２２に示す第３例は、図９，図１０を参照して説明した統合情報生成処理の第３例に対応しており、その統合情報生成処理の第３例で入手される可視情報（二次元情報）および秘密情報と同一の可視情報（二次元情報）および秘密情報が入手され、その統合情報生成処理の第３例で生成される署名鍵と同一の署名鍵が生成される。

【００９５】このように、秘密情報に基づいて、あるいは可視情報（二次元情報）と秘密情報とに基づいて、鍵情報を生成するシステムを構築すると、その鍵情報による署名により生成される署名情報のユニーク性を高めることができる。

【００９６】図２３は、検証処理の結果を示した模式図、図２４は、図１８に示す検証処理フローチャートに付加される部分フローチャートである。

【００９７】図２４に示す部分フローチャートは、図１８に示すフローチャートの比較処理（ステップＳ１０）の後の部分Ｐ２に挿入されるものであり、ここでは、比較処理（ステップＳ１０）の結果、統合情報２０から分離されたコンテンツ情報１０に署名処理を行なうことにより生成された検証用署名情報と、統合情報２０から分離された署名情報が一致した場合（ステップＳ１１）にのみ、ユーザによるコンテンツ情報のアクセスが許可され（ステップＳ１２）、不一致のときはそのアクセスは不許可となる（ステップＳ１３）。ここでいいうアクセスは、特定のアクセスにかぎられないが、例えば表示、プリント出力、送信等をいう。尚、このコンテンツ情報は署名情報とともに統合情報として一体化されており、したがってここでいうコンテンツ情報のアクセスは統合情報のアクセスを意味する。

【００９８】このように、検証により真正なコンテンツ情報であることが確認された場合のみアクセスを許可することにより、改ざんあるいはデータエラーの可能性のあるコンテンツ情報へのアクセスを防止することができる。

【００９９】

【発明の効果】以上、説明したように、本発明によればコンテンツ情報と署名情報が例えば表示画面上への表示あるいは用紙上へのプリント出力等の場合に、視覚的に一体化された統合情報に統合されているため、その統合情報として一体化された署名情報が、印影やサインと同様の役割りを果たし、ユーザに安心感を与えることができる。

【図面の簡単な説明】

【図１】本発明の情報管理装置の一実施形態を構成するパーソナルコンピュータの外観斜視図である。

15

【図２】図１に外観を示すパーソナルコンピュータのハードウェア構成図である。

【図３】ＣＤＲＯＭに記憶された情報管理プログラムの一例を示す図である。

【図４】本発明にいう情報管理プログラムが動作するもう１つの環境であるコンピュータネットワークを示す図である。

【図５】統合情報生成処理の第１例を示す模式図である。

【図６】統合情報生成処理の第１例を表わすフローチャートである。

【図７】統合情報生成処理の第２例を示す模式図である。

【図８】統合情報生成処理の第２例を実現するための、図６に示すフローチャートからの変更部分を示す部分フローチャートである。

【図９】統合情報生成処理の第３例を示す模式図である。

【図１０】統合情報生成処理の第３例を実現するための、図６に示すフローチャートからの変更部分を示す部分フローチャートである。

【図１１】統合情報生成処理の第３例の具体例を示す模式図である。

【図１２】統合情報生成処理の第３例のもう１つの具体例を示す模式図である。

【図１３】統合情報生成処理の第４例を示す模式図である。

【図１４】統合情報生成処理の第４例を実現するための、図６に示すフローチャートへの追加部分を示す部分フローチャートである。

【図１５】統合情報生成処理の第５例を示す模式図である。

【図１６】統合情報生成処理の第５例を実現するための、図６に示すフローチャートへの追加部分を示す部分フローチャートである。

【図１７】検証処理の第１例を示す模式図である。

【図１８】検証処理の第１例を表わすフローチャートである。

16

【図１９】検証処理の第２例を示す模式図である。

【図２０】検証処理の第２例を実現するための、図１８に示すフローチャートからの変更部分を示す部分フローチャートである。

【図２１】検証処理の第３例を示す模式図である。

【図２２】検証処理の第３例を実現するための、図１８に示すフローチャートからの変更部分を示す部分フローチャートである。

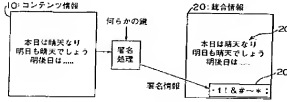
【図２３】検証処理の結果を示した模式図である。

【図２４】図１８に示す検証処理フローチャートに付加される部分フローチャートである。

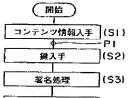
【符号の説明】

１０	コンテンツ情報
２０	情報処理プログラム
２０ａ	コンテンツ情報
２０ｂ	署名情報
２０ｃ	二次元情報
２０ｄ	付加情報
１００	パーソナルコンピュータ
１０１	本体部
１０１ａ	フロッピィディスク装填口
１０１ｂ	ＣＤＲＯＭ装填口
１０２	ＣＲＴディスプレイ
１０２ａ	表示画面
１０３	キーボード
１０４	マウス
２１０	ＣＤＲＯＭ
２１２	フロッピィディスク
２２１	中央演算処理装置（ＣＰＵ）
２２２	ＲＡＭ
２５０	情報管理プログラム
２５１	署名手段
２５２	統合手段
２５３	分離手段
２５４	検証用署名手段
２５５	比較手段
３００，４００	クライアントマシン
５００	サーバマシン

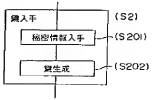
【図５】



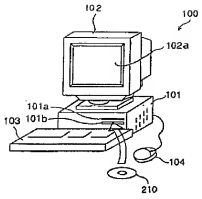
【図６】



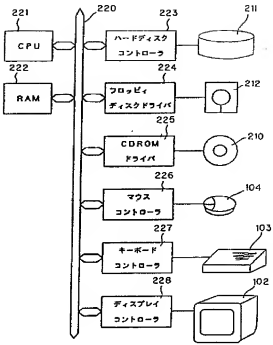
【図８】



【図１】

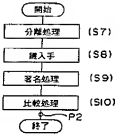


【図２】

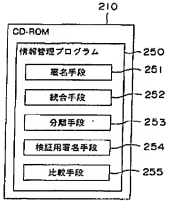


【図１４】

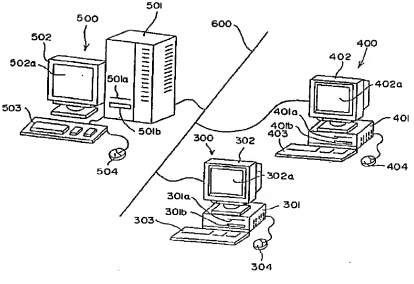
【図１８】



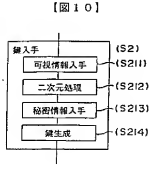
【図３】



【図４】

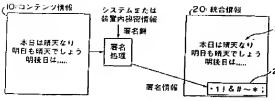


【図１０】

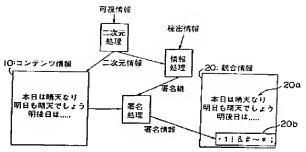


【図１６】

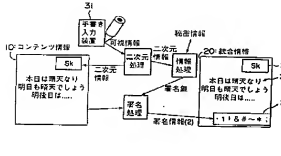
【図７】



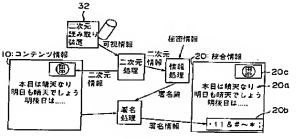
【図９】



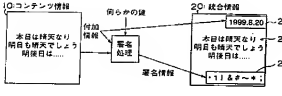
【図１１】



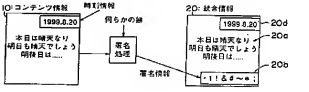
【図１２】



【図１３】

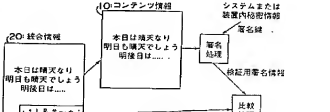


【図１５】

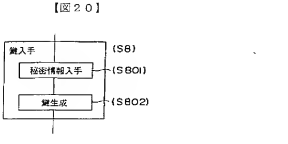


【図１７】

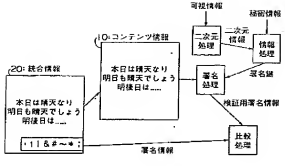
【図１９】



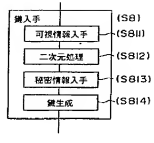
【図２０】



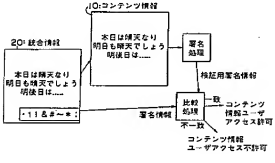
【図２１】



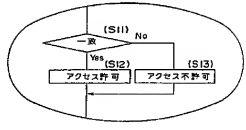
【図２２】



【図２３】



【図２４】



フロントページの続き

(72)発明者　秋山　良太
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　佐々木　孝興
東京都港区芝浦４丁目15番33号　株式会社富士通ビー・エス・シー内

Ｆターム(参考)　5B017 AA01 BA05 BA07 BB02 CA08 CA16
5C076 AA02 AA14 AA15 BA06
5J104 AA09 AA11 LA06 NA27
9A001 EE03 HZ28 JJ67 LL02